Volume 4, Issue 3, March 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Unique Technique for Clone Detection in Wireless Sensor Networks

T.Sangeetha, N.Jeba

Computer Science and Engineering ,
Anna University, India

Abstract— Wireless Sensor Networks where only a small number of packets need to be transmitted most of the time. So, an adversary easily captured and compromised the sensors which extract secret information from the captured nodes. As a result, an adversary may initiate a clone attack by replicating the captured nodes to extend the compromised areas employing clones. Due to the clone attacks, secret information, such as access keys, extracted from the captured nodes. For mobile WSNs, the clone detection schemes are classified into two types MCW and MDW according to their detection methods and detection ranges. This scheme provides effective solution for clone detection. But unlike static WSNs, in mobile WSNs, there are a few clone detection schemes that produce high detection errors. Due to the high detection errors in mobile sensor networks, there is a poor detection ratio in the clone detection methods. So, we introduce scheme using the Sequential Probability Ratio Test. which is used to detect the clone attack in WSNs by using Null Hypothesis technique.

Keywords— Clone attack, clone detection, replica attack, wireless sensor networks (WSNs).

I. INTRODUCTION

A Wireless Sensor Network is a group of specialized transducers with a communications infrastructure intended to monitor and record conditions at locations. A sensor network consists of multiple detection stations called sensor nodes; the transducer generates electrical signals based on sensed physical effects and phenomena. The transceiver, which can be hard-wired or wireless, receives commands from a central computer and transmits data to that computer.

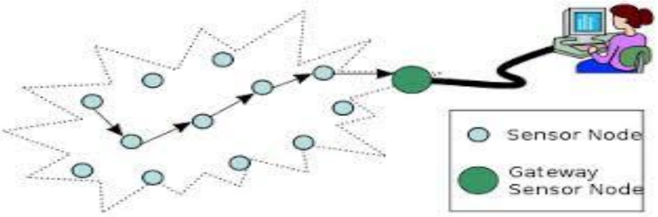

Fig 1.1 Wireless Sensor Networks

A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. In order to reduce the clone attacks in the wireless sensor networks the software based clone detection schemes is undoubtedly that they are not generic, meaning that their performance and effectiveness may depend upon their preconfigured network settings. So, the selection criterion is very important to detect the clone attacks in the wireless sensor networks. So, we first investigate the selection criteria of clone detection schemes. In addition to that to increase the detection ratio, so we introduce Sequential Analysis method. This scheme quickly detects mobile replicas with very small number of location claims.

II. TYPES OF CLONE ATTACK

A) Cloning Attack

Sensor networks allow to deploy large self-organized and adaptable sets of sensors for many applications used, unfortunately the simplicity and low-cost of the sensors eases cloning of compromised nodes by attackers. In such attack. An adversary uses the credentials of a compromised node to surreptitiously introduce replicas of that node into the network.. The detection of node replication attacks in a wireless sensor network is therefore a fundamental problem. Many protocols have been proposed in recent years for detecting node replication attack in sensor networks.

B) Node Replication Attack

In this type of attack (also known as clone attack) an attacker seeks to add a node to an existing sensor network by copying (replicating) the node ID of sensor node. A node replicated in this fashion can badly cut off a sensor network's performance: packets can be corrupted or even misrouted. If an attacker he can copy cryptographic keys to the replicated sensor an attacker loads its own nodes with the keys of and then deploys these cloned nodes in different locations of the sensor network.

C) Attacker model

This attack compromises between one or some network nodes and exploits their stored information and replicates a preferred number of nodes from a certain node with specific identity and places them in appropriate locations in network, so that respecting the desired goals, it will be able to make different attacks including, eavesdropping, inject fake data and attacking the network protocols. Also it is assumed that the attacker is not able to allocate a new identity to the clone nodes and mostly the attacker can only compromise a small part of the network nodes. Otherwise, with referencing to clone attacks costs, there is no need for node replicate.

Mobile-WSN (MWSN): In this network all of the nodes have mobile capability.

- WSN with mobile attacker sensor nodes are static but the attacker has mobile capability.
- WSN with mobile intrusion detection node, In this network all of the network sensor nodes are static but the intrusion detector nodes have mobile capability.

III. DEFINITIONS

CLONE DETECTION RATIO:

Definition: Clone detection ratio can be improved, Processing time of clone detection can be reduced, Total consumed energy can be reduced.

FALSE POSITIVE ERROR:

Definition: The error probability that a benign node is misidentified as replica node.

FALSE NEGATIVE ERROR:

Definition: The error probability that a replica node is misidentified as benign node.

DISTANCE FORMULA:

Distance calculates the one node to base station or sink node

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

SPEED FORMULA:

$$S = d/T$$

S- Speed
d- Distance from one node to another node
T-Time

IV. SEQUENTIAL PROBABILITY RATIO TEST

We apply SPRT to the mobile replica detection problem as follows. Each time a mobile sensor node moves to a new location each of its neighbours asks for a signed claim containing its location and time information and decides probabilistically whether to forward the received claim to the base station. Random walk starts, null and alternate hypotheses are defined in such a way that the null one is associated with the lower limit and the alternate one is associated with the upper limit. A random walk starts from a point between two limits and moves toward the lower or upper limit in accordance with each observation. On the other hand, each time the maximum speed of the mobile node is not reached, it will expedite the random walk to hit or cross the lower limit and thus lead to the base station accepting the null hypothesis that mobile node has not been replicated.

V. DUPLICATE NODE DETECTION

The nodes which are captured by an adversary can compromise the sensor nodes an make many replication This compromised nodes all have the same ID are present in the network. To understand the dangers of node compromise, we must first define what we mean by node compromise. Node compromise occurs when an attacker, though some subvert means, gains control of a node in the network after deployment. Once in control of that node, the attacker can alter the node to listen to information in the network, input malicious data, cause DOS, black hole, or any one of a myriad of attacks on the network. The attack arrayal so simply extracts information vital to the network's security such as routing protocols, data, and security keys. Generally compromise occurs once an attacker has found a node, and then directly connects the node to their computer via a wired connection of some sort. Once connected the attacker controls the node by extracting the data and/ or putting new data or controls on that node.

VI. PERFORMANCE EVALATION

Finally in this section we simulated the several representative clone detection schemes and evaluated them with the following performance metrics, i.e., total consumed energy, clone detection ratio, completion time, false positive error, and false negative error. In this section, we will briefly discuss how to design effective clone detection schemes in static and mobile WSNs. In the existing system we use clone detection method and in the proposed system we use fast and effective mobile replica node detection technique is used. Compared to the existing system we achieve high detection ratio in the proposed system.

VII. MOBILE REPLICA DETECTION USING SEQUENTIAL PROBABILITY RATIO TEST

This section presents the details of our techniques to detect replica attacks in mobile sensor networks. In static sensor networks, a sensor node can be considered to be replicated if it is placed at more than one location. However, if nodes are allowed to freely roam throughout the network, the above technique does not work because the mobile node's location will continuously change as it moves .Hence, it is imperative to use some other technique to detect replica nodes in mobile sensor networks. Fortunately, mobility provides us with a clue that can help resolve the mobile replica detection problem. Specifically, a mobile sensor node should never move faster than the system-configured maximum speed. Accordingly, if we observe that the mobile node's speed is over the maximum speed, it is then highly likely that at least two nodes with the same identity are present in the network. We propose a mobile replica detection scheme by leveraging this intuition.

VIII. SIMULATIONS OF CLONE DETECTION SCHEMES

A Simulation Environments and Scenarios Based on the aforementioned selection criteria, we conducted the simulation experiments on the representative clone detection schemes with regard to detection performance. For this purpose, we run the simulations in each scenario for a duration of 1000 s using a ns-2 network simulator .Each node uses IEEE 802.11 as a media access control protocol, in which the transmission range is 100 m, and the sizes of the areas covered by static WSNs and mobile WSNs are 1000 m × 1000 m and 500 m × 500 m, respectively. In order to determine the movement of mobile nodes, we employed the random trip mobility (RTM) model used in Ho's scheme as well. In the RTM model, each mobile node moves to a randomly chosen location .False positive error means an error of rejecting a null hypothesis when it is actually true. For instance, consider that the detection process for node *a* has produced a "positive" result (indicating that node *a* must be a clone), even though node *a* is actually not a clone. False positive error can be viewed as an error of excessive credulity. False negative error means an error of failing to reject a null hypothesis when it is not true.

IX. CONCLUSION

A Wireless Sensor Networks is used to sense and report the information to the end users. In that a clone attack is a critical problem. So, a clone detection schemes are used to detect the clone attack in the wireless sensor networks. We demonstrated our simulation results for the clone detection schemes representing different classification criteria. Then, we discussed how to construct the most effective clone detection scheme in WSNs. These schemes certainly need more restriction such as zone-based network in static WSNs, the results are reasonable and can guide us to choose proper schemes to achieve considerable energy savings. Such energy savings are highly enviable and frequently required in many ad hoc sensor network applications, such as monitoring emergency disaster notification data. In addition to that to enhance a detection ratio we use a technique called fast and effective mobile replica node detection scheme using the Sequential Analysis method. By using this method we achieve effective and robust replica detection capability with reasonable overheads.

REFERENCES

[1] Khanate Cho, Minho Jo, Member, IEEE, Taekyoung Kwon, Hsiao-Hwa Chen, Fellow, IEEE,and Dong Hoon Lee, Member, IEEE Classification and Experimental Analysis for Clone Detection Approaches in Wireless Sensor Networks. IEEE Trans. System journal., vol. 7, no. 1 march2013.

[2] SB. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, "Localize multicast: Efficient and distributed replica detection in large-scale sensor networks," IEEE Trans. Mobile Compute., vol. 9, no. 7, pp.913–926, Jul. 2010.

[3] K. Xing, F. Liu, X. Cheng, and D. H. C. Du, "Real-time detection of clone attacks in Wireless Sensor Networks," in Proc. *ICDCS*, 2007, pp. 3–10.

[4 J. W. Ho, M. Wright, and S. K. Das, "Fast Detection of replica node attacks in Mobile Sensor Networks using Sequential Analysis," in Proc. IEEE Int. Conf. Comput. Commun., Apr. 2009, pp. 1773–1781.

[5] International Journal of Scientific and Research Publications, Volume 2, Issue 11, November 2012 1 ISSN 2250-3153 www.ijsrp.org Classification and Analysis of clone attack detection procedures in Mobile Wireless Sensor Networks.

[6] B. Zheng, C.K. Lee, and W.-C. Lee, "Impact of Mobile Sink Speed on the Performance of WirelessSensorNetworks2008.

[7] H. Choi, S. Zhu, and T. F. L. Porta, "SET: Detecting node clones in sensor networks," in *Proc*. Security Privacy Commun. Netw. Workshops,2007, pp. 341–350.